Frequently Asked Questions (FAQs)

Things You Need to Know

Why is the DON changing the identification card?

The Common Access Card (CAC) is replacing the current DD Form 2 Geneva Identification Card because it will provide better physical and logical (computer) security as well as allow for a whole host of new applications that will streamline and improve the way we live and work. The DON in partnership with Department of Defense (DoD) has been testing the capability of smart card technology since the early 1990's. After a successful testing period during which the card proved to be an effective data storage device capable of securing information and access to networks and buildings, the Deputy Secretary of Defense (in memorandum dated 10 November 1999) directed that a smart card become the standard identification card throughout the DoD.

Who will receive the new ID card?

The new ID card is being issued to:

- Active Duty Uniformed Services Personnel
- Selected Reserves
- DoD Civilian Employees
- Eligible Contractor Personnel (on-site)

The new ID card is not currently being issued to:

- Family members
- Retirees
- Disabled American Veterans
- Inactive Ready Reserve
- Inactive Guard

These individuals will continue to use and receive the current ID card.

Frequently Asked Questions (FAQs)

What is the CAC being used for?

The DON is leading the way for the DoD, but since the CAC is going to be the standard military and Federal civil servant identification card, the other Services are also implementing the CAC. Below is a listing of some of the smart card applications currently in use.

- SmartImmune – Dam Neck, Great Lakes, Pensacola (Naval Training Commands)
- Smart Dental – Great Lakes, Dam Neck (Naval Training Commands)
- Manifesting and Tracking – Oahu, Korea (Exercise Foal Eagle 99), Thailand (Exercise Cobra Gold), future: Egypt (Exercise Bright Star 02)
- Warrior Readiness – Oahu
- Weapons Issuance – Marine Corps Base Hawaii, Oahu
- Food Service – Oahu, Great Lakes, Pensacola
- Quarterdeck Control – Selected ships
- Property Accountability – Selected ships
- Student Tracking/Visibility – Great Lakes
- ATM@Sea – Selected CVBG
- Recruit Advance Pay – Great Lakes

What is the Common Access Card (CAC)?

CAC is the title of the new smart identification and benefits card being issued throughout the DoD. It is the new standard ID card for active duty members of the Uniformed Services, Selected Reserves, DoD civilian employees, and eligible contractor personnel. The CAC will also be the principal card used to enable physical access to buildings and controlled spaces and for logical access to computer networks and systems. The CAC platform will contain the mandatory identification elements, physical and logical access capabilities, Public Key Infrastructure (PKI) authentication, encryption, digital signing certificates, and may also contain Department-wide and/or Component-specific applications such as manifesting, deployment readiness, food service, and medical/dental.

Do I have to get the new CAC?

Yes, provided that you are a member of the Uniformed Services, a civilian employed by DoD (not including members of the Intelligence Community), or a contractor who requires physical and/or logical access to the facilities and/or systems of the DoD. The CAC, which is the DoD's implementation of smart card technology, will be issued to over 1.3 million people in the DON over a two-year period. You will be notified by your command when you will receive a CAC; you may also receive a CAC as a replacement ID card when a new ID card is needed.

Frequently Asked Questions (FAQs)

Why a smart card for DoD?

Since 1993, the DoD has been conducting evaluations on smart card technology. Initially tested as an updateable individually carried data storage device, the Department's smart card mission has evolved to require an interoperable, backward compatible device for secure on-line data transfer and on-line transactions. In 1997, the Deputy Secretary of Defense (DEPSECDEF) established the Smart Card Technology Office to conduct a detailed evaluation during and oversee smart card demonstrations of joint applications on the island of Oahu. As the lead service, the DON (Navy and Marine Corps) played an important role in these evaluations. Subsequent tests were conducted at several Navy and Marine Corps bases using multiple and varied applications. The smart cards and applications tested by the DON at Dam Neck, Great Lakes, Pensacola, Oahu, Korea, and Thailand were largely successful. The success of these and other pilots and Service-specific demonstrations as well as the requirement to implement the DoD PKI using a secure hardware token (smart card) resulted in the November 1999 DEPSECDEF direction to use smart card technology for multiple applications on a single platform, the Common Access Card (CAC).

Why do the new cards look different from the current Uniformed Services identification card?

These cards are designed to display a minimum amount of printed information. You will note there is a great deal more information printed on the Geneva Conventions versions of the cards because of the information required to comply with the articles of the Geneva Conventions than on the cards issued to civilians within CONUS. This card also supports multiple functions - one of which is physical access/security. It has a vertical orientation consistent with many building passes.

Why is there no signature on the card?

There is no requirement for DoD to have a visible signature on its ID card from GSA, the State Department, or the Geneva Conventions; nor do any of the planned uses of the card within DON require a signature. Consequently, the signature was not included on the card. However, certificates for digitally signing electronic transactions will be included on the CAC. These certificates will be used to gain access to PKI-enabled services.

Frequently Asked Questions (FAQs)

What will my CAC be used for?

At a minimum, the CAC will be the standard ID card for eligible members of the Uniformed Services, DoD civilian and eligible foreign national employees, and eligible contractor personnel. It will be the principal card used to enable physical access to buildings and controlled spaces, will facilitate a standardized, uniform approach to access DoD facilities and DoD computer systems; and will carry public key infrastructure (PKI) identity, email, and encryption certificates.

In addition to the DoD-mandated functionality, the CAC is being integrated into the coming Navy Marine Corps Intranet (NMCI) infrastructure. The CAC will be the access token used to support NMCI network logon and will serve as the PKI token for digitally signing and encrypting email.

The CAC is capable of a variety of functions, most of which will be added in the future as applications are approved at both the DoD and DON levels. One advantage of using smart card technology as the new identification card is to support multiple applications with a single card. Once initial issuance has been accomplished, the technology will be exploited by the DON with the potential to greatly improve business processes, mission effectiveness, and quality of life.

Where will the CAC be issued?

The CAC will be available at your local DEERS/RAPIDS site sometime in the next two years. Upgrades to the current DEERS/RAPIDS stations are scheduled to occur between now and October 2002. As these sites are upgraded and staffed for issuance, you will receive information about the time, place, and procedure for obtaining a new card through the established command networks. Card issuance will be tailored to meet the needs of each issuing station, and the procedure will be similar to the method used to issue current ID cards. Military personnel will continue to go to their local Personnel Support Detachments (PSDs) or Consolidated Administration Centers for their cards. The PSDs at locations that support large civilian or contractor populations will be augmented by additional issuance stations in security or badging offices and other suitable locations.

Frequently Asked Questions (FAQs)

When I visit a RAPIDS site for CAC issuance, what should I bring with me?

All military and civilian employees (including appropriated and non-appropriated funded and direct and indirect hire foreign nationals) must bring the following:

1. A Picture ID;
2. Your Government email address if you use a government computer: (Be sure to print clearly your full unclassified Internet email address (not your display name). Your computer system administrators can assist you with documenting your email address. If you bring the wrong address and/or it is entered incorrectly, you will have to return it later to correct it. Personal email addresses (e.g., AOL accounts) will not be accepted.)
3. A six (6) to (8) digit number to use as a Personal Identification Number (PIN). It should not be a number derived from something easily known about you, such as part of your SSN, birthday, anniversary date of you or a family member, telephone number, or address.

New DoD Civilians Employees, Government Contractors, or others not listed must bring the following:

1. Two Picture Ids
2. Your government email address
3. A six (6) to eight (8) digit number to use as PIN
4. A completed and signed DD 1172-2

When will the CAC be available?

Testing of the new system that generates the cards began in October 2000. Selected Beta test sites are issuing CACs at this time. Issuance of the CAC will begin worldwide, as sites are upgraded, beginning in May 2001.

Where can I use my CAC?

The uses of the CAC depend on the Component/Command that you support. Each Component can customize the CAC to meet their specific needs. Some possible uses of the card might include manifesting, building access, network access, food service, training, dental, medical, and physical/logical access. Many more applications are being developed.

Can I use the CAC overseas?

Yes. Your CAC replaces your current DD Form 2 ID card and will be used overseas just as the old ID card was.

Frequently Asked Questions (FAQs)

When will I need to get a new card?

The goal is to issue cards to all eligible DON personnel with the appropriate PKI credentials by the end of FY02. In addition, all NMCI users should have a CAC on or before NMCI cut-over at their respective sites.

The lifecycle for a normal expiration of the CAC is three years, or the end of your active Navy or Marine Corps service. In accordance with card expiration dates, a new card should be issued to update the printed and stored data on the card.

How will I be issued a CAC if I am a Reservist who goes on active duty?

Reservists will be issued a new CAC when they go on active duty for more than 30 days; the CAC will have an expiration date of three years or the end of their duty, whichever comes first. They will retain their Reserve CAC.

When would I be required to update the information on the CAC?

The requirement to update the information on your CAC will depend on the Component/Command you support.

Will the CAC replace the current Uniformed Services ID card?

Yes, for those populations targeted for issuance. The CAC will replace DD Forms 2, 2764, 2765, and 2750 for members of the eligible populations. The initial issuance of the CAC will not include the Individual Ready Reserve (IRR), the Inactive National Guard (ING), the Standby Reserve, the Retired Reserve, or retired members of the Uniformed Services. These populations will continue to be issued the present Uniformed Services identification card (DD Form 2).

There will be no change for Uniformed Services family members who will continue to be issued DD Form 1173 or DD Form 1173-1. The CAC will replace DD Form 2765 for DoD civilians and eligible contractor personnel. However, DD Form 2765 will continue to be issued to all other eligible personnel.

Will currently issued DD Forms 2, 2764, 2765, and 2750 still be valid?

Yes. DD Forms 2, 2764, 2765, and 2750 are the current military identification cards, and until they are replaced by a CAC and phased out, they will still be valid. This will happen gradually as they expire or are replaced, and as the CAC implementation progresses. DD Forms 2 and 2765 (Reserve, Reserve Retired, and Retired) will continue to be issued to eligible populations that are not eligible for the CAC.

Frequently Asked Questions (FAQs)

Will currently issued DD Forms 1173 and 1173-1 still be valid?

Yes. There is no CAC replacement for these ID cards at this time. They will continue to be issued to their eligible populations and they will continue to be valid.

Will personnel or medical records be carried on the CAC?

There is no need to carry complete personal or medical records on the card. The CAC is designed to improve the security of access to those records. Selected personal and medical information may be placed on the card in secure data "containers" to support service or component-specific applications. This will be done only if approved through the Configuration Management process both internally within DON and by the Smart Card Senior Coordinating Group within the DoD. The CAC's integrated circuit chip (ICC) will be used initially only to store the keys and certificates required for secure on-line data transfers and basic personnel and demographic data.

Will benefits and privileges change for individuals eligible for the new cards?

No. The benefits and privileges will be the same as those conveyed with the DD Forms 2 (Active or Reserve), 1173, 2750, 2764, and 2765.

Will the CAC be issued to any new categories of individuals who were not eligible to receive current DoD ID cards?

Yes. The CAC will be issued to US-based civilians and eligible contractors determined by their contract administrators to need access to facilities and computer systems.

Are civilians stationed within the US going to be able to use the Commissary and Exchange now with the new cards?

No. The CAC does not change the status of an individual; it merely documents it.

Are Uniformed Services' dependents and retirees eligible for the Common Access Card (CAC)?

No, not at this time. All Uniformed Services' dependents will continue to be issued the DD Form 1173 or 1173-1, and retirees will continue to be issued the DD Form 2 (Retired, Reserve Retired).

Will any of the manually prepared (i.e. typewriter generated paper) ID cards remain in circulation and will they continue to be valid?

Yes, until the CAC is fully fielded for the DD Form 2 (Active and Reserve) and the DD Forms 1173, 2750, 2764, and 2765 for those eligible for a CAC. Existing paper DD Forms 2 (Retired), 1173 (for dependents of members of the Uniformed Services and

dependents of civilians overseas), and 1173-1 will continue to be in circulation along with the machine-generated RAPIDS versions.

TECHNICAL QUESTIONS

What is a smart card?

A smart card refers to a credit card-size device (approximately 2.25" x 3.625") that contains one or more integrated circuit chips and may also employ one or more of the following technologies:
1) Magnetic stripe;
2) Bar codes, linear or two-dimensional;
3) Non-contact and radio frequency transmitters;
4) Biometric information;
5) Encryption and authentication; and/or
6) Photo identification.

A smart card stores and processes information on an integrated, microprocessor chip located within the body of the card. This chip can hold a variety of information, from stored (monetary)-value used for retail and vending machines, to secure information and applications for operations such as secure access to computer systems. New information and/or applications can be added depending on the chip's capabilities and storage capacity.

In general, different types of smart cards being used today are contact, contactless, combination, memory, and microprocessor cards.

- Contact smart cards must be inserted into a smart card reader. These cards have a contact plate on the face, which makes an electrical connection for reading from and writing to the chip when inserted into the reader.
- Contactless (proximity) smart cards have an antenna coil, as well as a chip embedded within the card. The internal antenna allows for communication and power with a receiving antenna from the reading device to transfer information. Close proximity is required for such transactions, which can decrease transaction time while increasing convenience.
- A combination card functions as both a contact and contactless smart card.
- A memory card has storage capability, and an input/output interface, but no processor. Memory cards do not offer a high level of security because the card has neither the intelligence capable of reacting to an undesirable intrusion nor the processing capacity to support security algorithms.
- A microprocessor card houses nothing less than a microcomputer. The chip on a microprocessor card can have an area of up to 25 mm2. The chip underlying the gold button is linked to the plastic via five standard contacts. Microprocessor cards support cryptographic algorithms and security mechanisms.

The Common Access Card (CAC) is a contact smart card. The CAC follows the ISO 7816 standard for integrated circuit cards (ICC) for electrical contact. The integrated microprocessor chip can coexist with other types of technology on a single card. The CAC contains an ICC containing 32K of data storage and memory (EEPROM), a linear (Code 39) bar code, a two-dimensional (PDF 417) bar code, a magnetic stripe, and a color digital photograph. Multiple technologies exist on the CAC to accommodate the migration of multiple applications using the existing bar code and magnetic stripe reader infrastructure until the new smart card ICC reader technology is in place. The CAC will be a commercially derived solution and will follow commercial standards to the greatest extent possible. Using multiple technologies on a single card also enables an organization to make a cost-effective transition to smart cards using existing magnetic stripe and bar code infrastructures until the smart card infrastructure is in place.

What are the benefits of smart cards over magnetic stripe cards?

Smart cards containing an integrated circuit chip have the capacity for greater storage space than traditional magnetic stripe cards. Smart cards are more reliable, perform multiple functions, and are more secure because of high security mechanisms such as advanced encryption and biometrics. Due to the card's self-contained processing capabilities, smart cards can enable local, or off-line, transactions between the card and host terminal or computer. Unlike most portable data storage media, information residing on the chip can be continually updated or modified.

Frequently Asked Questions (FAQs)

What information will be stored on the CAC?

Smart cards only contain selected, abbreviated data relating to a person's work functions or benefits and privileges. Sensitive data such as passwords or highly personal medical information are not contained on an individual's smart card. A multi-application smart card is geared towards making the cardholder's life easier.

Each card will have printed textual information, a color photograph, an ICC, magnetic stripe, and two bar codes. However, the front and back of the CAC will vary slightly according to the type of card holder. There are four portable storage media on the CAC: an ICC, Code 39 bar code, PDF 417 bar code, and magnetic stripe. The ICC will hold most of the data on the card while the two bar codes and magnetic stripe store the rest of the information. The information stored on the ICC includes:

- Card expiration date;
- Card security code;
- First, middle, and last name;
- Gender;
- DoD EDI person identifier;
- Government agency;
- Branch of Service;
- Pay grade;
- Rank;
- Date of birth;
- Meal entitlement code;
- Commissary code;
- Pay Category
- Direct care benefit type code;
- Entitlement condition.
- Card issuance date;
- Demographic date chip expiration date;
- Name suffix;
- Person designator;
- Blood type;
- Non-Government agency;
- Duty status;
- Non-medical benefits end calendar date;
- PKI functionality (3 certificates and key identifiers);
- DoD contractor function code;
- Exchange code;
- MWR code;
- Civilian Health Care entitlement type code;
- Medical benefits end date; and

In addition, the ICC will be partitioned to leave adequate storage space for each specific Component's use. Additional information can be stored on the ICC depending on the Component and its needs.

The Code 39 bar code will contain the following data elements: a person identifier, DoD EDI identifier, calendar date for end of medical benefits, branch of Service, and duty status.

The PDF 417 will contain the following data elements: an identifier to link a card to a user; PDF 417 version, person identifier (SSN, foreign ID, etc.); user last name; DoD EDI identifier; date of birth; civilian health care entitlement code; end date of medical benefits; branch of Service; duty status; pay category; and pay grade.

Lastly, the magnetic stripe will store the following data elements: card holder's SSN, Government Agency code, and physical security information.

Frequently Asked Questions (FAQs)

What is Public Key Infrastructure (PKI) and how will the CAC use PKI?

PKI is the basic framework and services that are being put in place within DoD to ensure information systems security. It provides the capability to attach digital signatures to electronic documents and to encrypt and decrypt electronic documents for secure transmission. The CAC will serve as the user's PKI token, which means that the chip located on the CAC will be used to store the user's private key identity, email, and encryption certificates. These certificates are used to gain access to PKI-related services.

The DON supports several small-scale PKI projects, but implementation of the CAC and the Navy Marine Corps Intranet (NMCI) will initiate the first Navy-wide digital signature functionality. The digital signatures, email encryption, and secure access to web servers and networks enabled by the certificates loaded on the card will secure information, reduce the dependency on paper and paper-based processes, and positively identify individuals in an electronic environment.

Can I see the information that is stored on the card?

Just as you cannot "see" the information stored on the magnetic stripe of your credit card, you cannot see the information stored on the card. The information on the chip is compressed and securely stored. Access to each data element is limited to approved applications, ensuring that the appropriate individuals/networks can read only the information they need. As CAC applications become more common, additional functionality, such as reviewing and updating information on the CAC by the individual, may become available.

Who has access to the information?

Only individuals who have authorization to perform normal identification processes and run CAC applications have access to the information on your CAC. For example, if your card contains dental information, only someone who has an authorized application and "need to know" can access and review the data in your dental file. Each application on the CAC is firewalled from the other and someone who has access to one application does not typically have access to another application.

Each application can be secured with different levels of protection. Some applications can have encrypted levels of security while others may not have any encryption at all. The ability to read a file does not necessarily mean that the person has the ability to alter the information in a file.

CAC holders can release their information using their personal identification number (PIN) at RAPIDS stations or at facilities using CAC applications.

Frequently Asked Questions (FAQs)

Who has the capability to make changes to my card?

Only authorized personnel with legitimate applications will have the capability to make changes to your card. The applications approved by DoD and DON will grant a finite number of personnel access to certain data elements predetermined to be necessary for that particular application to run. In order to change these elements, you will have to provide your PIN and will, therefore, have full cognizance of the transaction.

What differentiates the cards with privileges from ones that don't have them?

The cards with privileges have an "Authorized Patronage" section on the front of the cards where the privileges are listed.

Can someone assume my identity if they find my smart card? Can they access the information stored on the smart card?

No. The CAC is designed to make it even more difficult for someone else to steal information or assume your identity than the present card. An integrated chip is more secure than any other card technology. It is very difficult for anyone to access the information on your smart card without the proper identification, applications, and submission of your personal identification number (PIN).

If you lose a credit card, someone can find it and use it to make purchases with little difficulty. However, a smart card, which has your photo on the front, is more difficult to use than a credit card. Not only would an individual need the card and resemble the person on the card, but they will need a PIN to use it. This is why it is imperative that the PIN be kept in a secure location, not written on the back of the card or left out in plain view. The CAC is also more tamper-resistant than the current ID card.

The PKI certificate stored on the card provides an additional security feature. While the card is in your possession, the PKI token authenticates the cardholder, ensures the integrity and confidentiality of any data your transmit, and prevents you from denying or disowning completed transactions. However, these certificates can be revoked whenever necessary, preventing individuals with stolen or "borrowed" cards from using the cards. Once a certificate is revoked, transactions enabled by that card are no longer validated or accepted by receiving parties; this is the equivalent of canceling a stolen credit card. For this reason, a lost or stolen card should be reported immediately.

What do I do if I misplace or lose my CAC?

Report the missing card to your supervisor or security officer as soon as possible, and return to an issuance site for a replacement card.

Frequently Asked Questions (FAQs)

What do I do if I forget my PIN?

If card holders forget their PIN they can go to the nearest issuance site where they will be given the opportunity to prove they are the owner of the card by matching their fingerprint against the fingerprint that was stored on DEERS when they were issued the card. If the fingerprint matches successfully, a new PIN can be selected.

Your PIN should be stored in a secure location away from the card for just this reason. If you enter the incorrect PIN three times consecutively, the card is designed to lock you out.

Where is the information coming from to populate the CAC?

The information written to the CAC comes from data in the Defense Enrollment Eligibility Reporting System (DEERS). This information comes from the same source as the old ID card.

Can these new cards be prepared manually?

No. The new cards are only available as produced via RAPIDS workstations. There are no other versions of these cards available. Furthermore, it is illegal to produce cards through any procedure not approved and conducted through the Department of Defense.

What do I do if I lose my CAC? What happens if I lose my CAC on travel?

Report the missing card to your supervisor, security advisor, or the nearest DEERS/RAPIDS issuance site as soon as possible. Your card will be "cancelled," all private keys, certificates, benefits, and privileges will be revoked, and a new CAC will be issued to you at your local DEERS/RAPIDS station. If you are traveling, your local DEERS/RAPIDS station should be able to refer you to the nearest issuance site.

What is the benefit of smart card technology for the Navy?

The Department of the Navy has been a leader in conducting pilots using smart card technology since 1997. Detailed testing of the cards and their capabilities has proven them an effective technology capable of reducing costs, strengthening information security, reducing paperwork and redundant data entry, and improving mission readiness. Overall, implementation of the CAC is expected to streamline business processes and enable the Navy to both protect and share its information more effectively and efficiently. The card's ability to support multiple applications and multiple technologies will reduce the number of cards issued, an important improvement in quality of life.

Frequently Asked Questions (FAQs)

What is contained in the ISO 7816 standard?

The International Standards Organization (ISO) facilitates the creation of voluntary standards through a consensus-building process that is open to interested participants. ISO 7816 is the set of international standards for ICC (commonly known as smart cards) that use electrical contacts. Anyone interested in obtaining a technical understanding of smart cards should become familiar with what the ISO 7816 standard covers as well as what it does NOT cover.

ISO 7816 does not address smart card applications. Most current and planned applications require custom files and coding. However, there are efforts underway to create common application standards. The most prominent current example is the cooperative development of financial payments standards by Europay International, MasterCard International, and Visa International (EMV).

Source: SCIA homepage: http://www.scia.org/

What are the benefits of smart cards over other types of memory storage cards?

The ICC technology on a smart card is more advanced than magnetic stripe technology and other portable storage media, such as bar codes. The ICC technology has thousands times greater storage capacity than traditional magnetic stripe and bar code technologies. Information on a magnetic stripe is easily accessible and can be duplicated easily, whereas an ICC is very secure. In addition, smart cards are more reliable, perform multiple functions and are more secure because of high security mechanisms, such as advanced encryption and biometrics. Due to the ICC's self-contained processing capabilities, smart cards can enable local, or off-line, transactions between the ICC and host terminal or computer. Unlike bar codes and most portable data storage media, information residing on the ICC can be continually updated or modified.

Why will the CAC include bar codes and a magnetic stripe in addition to the ICC?

Bar code and magnetic stripe media are required for backward-compatibility with existing applications, and to give the sponsors of these applications time to migrate to smart card technology.

What types of media will be included on the CAC?

The media on the CAC includes an ICC, a linear (Code 39) bar code, a two-dimensional (PDF 417) bar code, a magnetic stripe, a color digital photograph, and printed text.

Frequently Asked Questions (FAQs)

What applications will be included on the CAC's ICC?

Initially, the CAC's ICC will include minimal demographic data; identity, signature e-mail, and encryption e-mail certificates (PKI); data elements pertaining to benefits (e.g., commissary and exchange codes); organization and rank information; and data to assist in card management (e.g., issue date, expiration date). Applications under consideration for future implementations include deployment readiness, food service, financial (e.g. stored value, electronic purse, ATM), manifesting, medical and dental, student visibility, armory and property accountability, training, and rifle range.

What are Code 39 bar codes and PDF 417 bar codes?

Code 39 is one of the most popular bar code types used in industry today. Code 39 encodes 43 data characters (0 through 9, A through Z, 6 symbols, and a space); three of the nine elements are wide and six are narrow elements. This code is also referred to as Code 3x9 or Code 3 of 9.

Portable Data File (PDF) 417 is a stacked, two-dimensional bar code type consisting of 17 modules each containing 4 bars and spaces. This type of bar code can be read with a handheld laser or CCD scanners. The code structure for a PDF 417 allows between 1000 to 2000 characters per symbol with an information density of between 100 and 340 characters. Each symbol has a start and stop bar group which extends the height of the symbol.

The choice of bar code depends on the kind of data you want to encode.

Source: www.adams1.com/pub/russadam/stack.html

What information is contained on the Code 39 and PDF 417 bar codes?

The Code 39 or linear bar code contains a total compressed storage of 18 bytes of data. The Code 39 bar code contains the Electronic Data Interchange (EDI) personal identifier, a CAC holder's social security number (SSN), Uniformed Service Branch, and some card management data tools. The PDF 417 bar code contains a total compressed storage of 60 bytes of data. The PDF 417 bar code holds minimal personal data, benefits information (date of birth and entitlement conditions), organizational information, and some card management data tools. The data contained on the Code 39 and PDF 417 bar codes is required for use in legacy (existing) applications.

What are the smart card architecture requirements for the CAC?

CAC Architecture	Recommendation
Card Operating System	√ Java Card 2.1 plus with Sun Certified Virtual Machine

Frequently Asked Questions (FAQs)

CAC Architecture	Recommendation
Standards:	√ ISO 7816, 1-7 √ T=0, T=1 √ EMV √ Global Platform 2.0 with Global Platform Certification. Preference given to proposals Delegated management as well as Delegated Services (i.e. loading, installation, deletion, etc) per the Open Platform specifications √ Java Card 2.1 or higher Certified
Micro-controller/Processor:	√ Minimum: 32K micro-controller (with 32K EEPROM with a minimum of 22K EEPROM space available) √ Minimum: 8-bit processor √ Must contain a cryptographic co-processor
Card Functionality (Available EEPROM will contain):	√ DoD Provided Data Applet √ DoD Provided PKI Applet capable of generating and storing 3 Digital Certificates and associated key pairs √ Minimum R/W cycles: 100,000
<u>Cryptography:</u> Encryption Algorithms: Digest Algorithms: Key Exchange Algorithms: Signature Algorithms:	√ DES √ Triple DES √ Skipjack (Optional) √ SHA-1 √ MD5 (Optional) √ RSA √ RSA, PKCS#1 Format ✓ Minimum support 1024 bit key length ✓ Hardware Random Number Generation √ FIPS 180-1 Secure Hash Standards √ FIPS 186-1 Digital Signature Standards
On Card Key Generation Performance Criteria:	√ Preference given to proposals providing x=30 seconds
Security:	✓ Minimum: FIPS 140-1, Level 1 Certification for entire card platform ✓ Provide information on (both hardware and software) protection techniques used to combat Differential Power Analysis and Simple Power Analysis attacks ✓ Seal/protection of the integrated circuit as well as

CAC Architecture	Recommendation
	complete audit controls on all semiconductors to include scrap reports and 100% reconciliation. ✓ Power line emanations: Minimum information leakage measure; functional information being leaked out of the power lines should be at least 50% masked with random power fluctuations." If the vendor's card cannot meet this threshold, then the vendor shall provide information of both hardware and software protection techniques used to combat Differential Power Analysis and Simple Power Analysis Attacks."

How will the space on the CAC's ICC be allocated?

Based on the DoD functionality, backward compatibility, and card architecture and platform, the following allocation table has been approved for the CAC:

CAC Functionality	Space	Overhead	Total
DoD: Data Elements (Maximum Space)	0.2 Kilobytes	2.2 Kilobytes	2.4 Kilobytes
DoD: PKI (Maximum Space)	8.3 Kilobytes	2.0 Kilobytes	10.3 Kilobytes
Enhancement to CAC Platform (Maximum Space)	10.0 Kilobytes	N/A	10.0 Kilobytes
Component Specific Area (Minimum Space)	7.0 Kilobytes	N/A	7.0 Kilobytes
Total	**25.5 Kilobytes**	**4.2 Kilobytes**	**29.7 Kilobytes**

Is there a backup of the data on the CAC?

Yes, it is contained in DEERS. In addition, the Certificate Authority escrows the public keys and the private key for encryption.

Will the NMCI initiative affect issuance of the CAC?

Yes. An integral component of the basic services provided within NMCI are those functionalities enabled by the use of the DoD PKI and smart card technology – network logon, electronic signature, and encryption. Under the requirements of the NMCI contract, DON is responsible for providing the CAC to facilitate and enable these functions.

The NMCI implementation schedule, in particular, has an impact on issuance of the CAC. It is the DON's goal that all NMCI users at any given base have a CAC on or before the date NMCI is launched at that location. Therefore, the DON issuance strategy is closely integrated with NMCI deployment.

GENERAL QUESTIONS

Where can I go to find out more information about the CAC?

To find out more information about the new CAC, please visit the following sites:

- Department of the Navy's Smart Card Office website at http://www.donsmartcard.com
- Department of the Navy Central Information Officer website at http://www.donim-it.navy.mil
- Department of Defense's Access Card Office's website at http://www.dmdc.osd.mil/smartcard
- Look for brochures at your local exchange, information on your Leave and Earnings Statement or through message traffic, broadcasts on American Forces Information Network, and press releases

What is the worldwide distribution of smart cards and what applications are prevalent geographically?

Smart cards are most prominent in Western Europe, which held 70% of the market in 1996. Worldwide distribution is:**

Region	1996	2000
North America	3%	12%
South America	11%	10%
Western Europe	70%	40%
Asia	10%	30%
Rest of World	6%	8%

**Source: Phoenix Planning & Evaluation

Source: Smart Card Industry Association (SCIA) homepage: http://www.scia.org/

Frequently Asked Questions (FAQs)

Who can I contact for more information on the Department of the Navy's smart card/CAC Program?

To find out more information about the new CAC, please visit the following sites:

- Department of the Navy's Smart Card Office website at http://www.donsmartcard.com
- Department of the Navy Central Information Officer website at http://www.donim-it.navy.mil
- Department of Defense's Access Card Office's website at http://www.dmdc.osd.mil/smartcard
- Look for brochures at your local exchange, information on your Leave and Earnings Statement or through message traffic, broadcasts on American Forces Information Network, and press releases

Where are people using smart cards?

Smart cards are being used by numerous private and public sector organizations to improve business processes. Businesses and governments worldwide use smart cards for applications in banking, health care, transportation, logical and physical access, loyalty programs, and military operations. A sampling of the different programs being implemented worldwide includes:

- United States – In 1999 American Express began issuing a smart card credit card, called Blue, that can be used for making secure on-line credit card purchases via a computer with a smart card reader attached.

- Spain - Consumers in Spain are using Visa Cash, and it's so popular that it's used and accepted throughout the country in telephones and mass transit. In addition, the National Mint is leading the CERES (Spanish Certification) project which establishes a Public Certification Authority that will ensure and authenticate the confidentiality of communications through open communication networks between citizens, companies, or other institutions and public administrations.

- Argentina - Visa Smart Debit and Visa Cash on a single card was introduced in January 1996. Today, Visa Cash can be used to pay for meals at McDonald's fast food outlets and at other merchants, such as video rental stores, newsstands, gas stations, and convenience stores.

- Barrie, Ontario, Canada - Consumers and college students were recently introduced to Visa Cash, the convenient replacement for cash. They're using smart cards at merchant locations throughout the city and on university campuses.

- Brazil - Visa Cash was introduced to consumers in December 1996. Since then, consumers have been actively using their Visa Cash smart cards at a wide variety of merchant locations, including fast food restaurants, bakeries, newsstands,

convenience stores, and cafeterias. It is one of the most successful Visa Cash programs in the world.

- France - Carte Bancaire has delivered 22 million cards. The chip is used to authenticate the card dynamically.
- France - Telecarte, the first large-scale stored value chip card application. The chip contains just the memory.
- France - Over 100 million smart cards are used in pay phones around the country.
- Germany – Over 78 million smart cards (memory cards) were personalized and mailed to German citizens as a health insurance card.
- Hong Kong - Consumers are using Visa Cash enthusiastically as a replacement for cash. It's accepted in a wide variety of merchant locations, and it's one of the fastest growing Visa Cash programs.
- Philadelphia, Pennsylvania, USA – All Villanova University students use a smart card (known as Wildcard) as an identification (ID) card, meal card, library card, access card to dorms, classrooms, and labs, debit card, and an ATM card.
- Russia - Consumers are using a version of the Visa Smart Debit and Visa Smart Credit card, adapted for parts of the world where telecommunications may be limited, yet a secure method of transaction authorization is required.
- San Francisco, California, USA - Employees at Bank of America and Visa are using Visa Cash on the Internet for small-value purchases. Employees at Visa headquarters have been using Visa Cash in their cafeteria since April 1995. Employees at Bank of America use a multi-application smart card for door access, personal computer access, file encryption, and Visa Cash.
- Singapore, Hong Kong, Taiwan - Consumers are using a Visa Smart Credit card that tracks a loyalty program for various merchants.

Source: VISA homepage: http://www.visa.com/nt/chip/info.html, American Express: http://home4.americanexpress.com/blue/faq_chip.asp, Spanish Public Certification Authority http://www.cert.fnmt.es/ingles/que.htm, and Villanova University: http://unit.villanova.edu/wildcard/homepage.htm